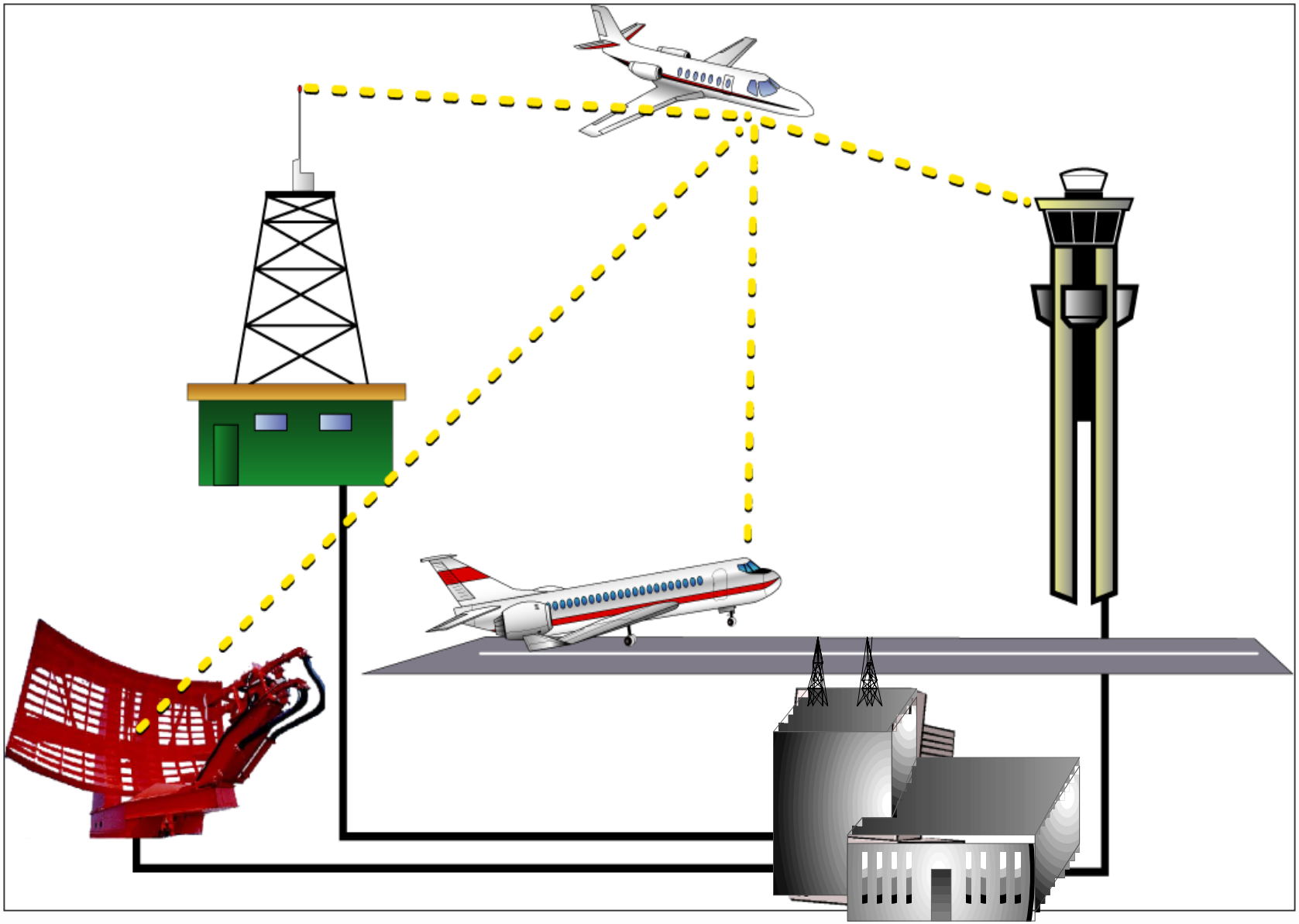
An Approach to the Software Aspects of Safety Management

Ron Stroup
FAA, Office of Information Services
Process Engineering Division, AIO-200
Software Safety and Certification Lead
PH. (202) 493-4390
Ronald.L.Stroup@faa.gov
www.faa.gov/aio

National Airspace System (NAS)



FAA Experience (1/2)

- What were our concerns?
  - Ineffective Risk Management.
  - Immature software acquisition processes.

GAO Report - Air Traffic Control: Immature Software Acquisition Processes Increase FAA's System Acquisition Risks. AIMD-97-47, March 1997

FAA Experience (2/2)

- How are we improving?
  - Ineffective Risk Management
    - Develop safety risk management policy.
      (FAA Order 8040.4 Safety Risk Management)
      (Software Safety and Certification Initiative)
    - Improve knowledge of systems engineering.
      (Systems Engineering Council)
  - Immature software acquisition processes.
    - Improve knowledge of software engineering.
      (Software Engineering Body of Knowledge)
    - Develop software policy, practices, and technologies.
      (FAA integrated Capability Maturity Model)

Order 8040.4 Safety Risk Management

- **Purpose**
  - Established safety risk management policy
    - Formalized process for all high-consequence decisions.
  - Prescribes procedures for implementing safety risk management and decision-making tool
    - Plan, Identify, Analysis, Assess, Decision
  - Establishes Safety Risk Management Committee
    - Provides advice, counsel the organizations

Safety Risk Management Committee

- Provides supplemental support to assist in the overall risk analysis capability and efficiency of key FAA organizations
- Maintains a risk management resource directory
  - Risk methodologies employed
  - Resource assistance
- Identifying suitable risk analysis tools and training

FORMALIZE A COMMON SENSE APPROACH

System Engineering Council

- **Purpose**
  - Orchestrates common systems engineering activities across the NAS
  - Responsibility, authority, and accountability for the development, documentation, deployment, control, and monitoring of the systems engineering process.
- **Products**
  - System Engineering Management Plan
  - System Engineering Manual

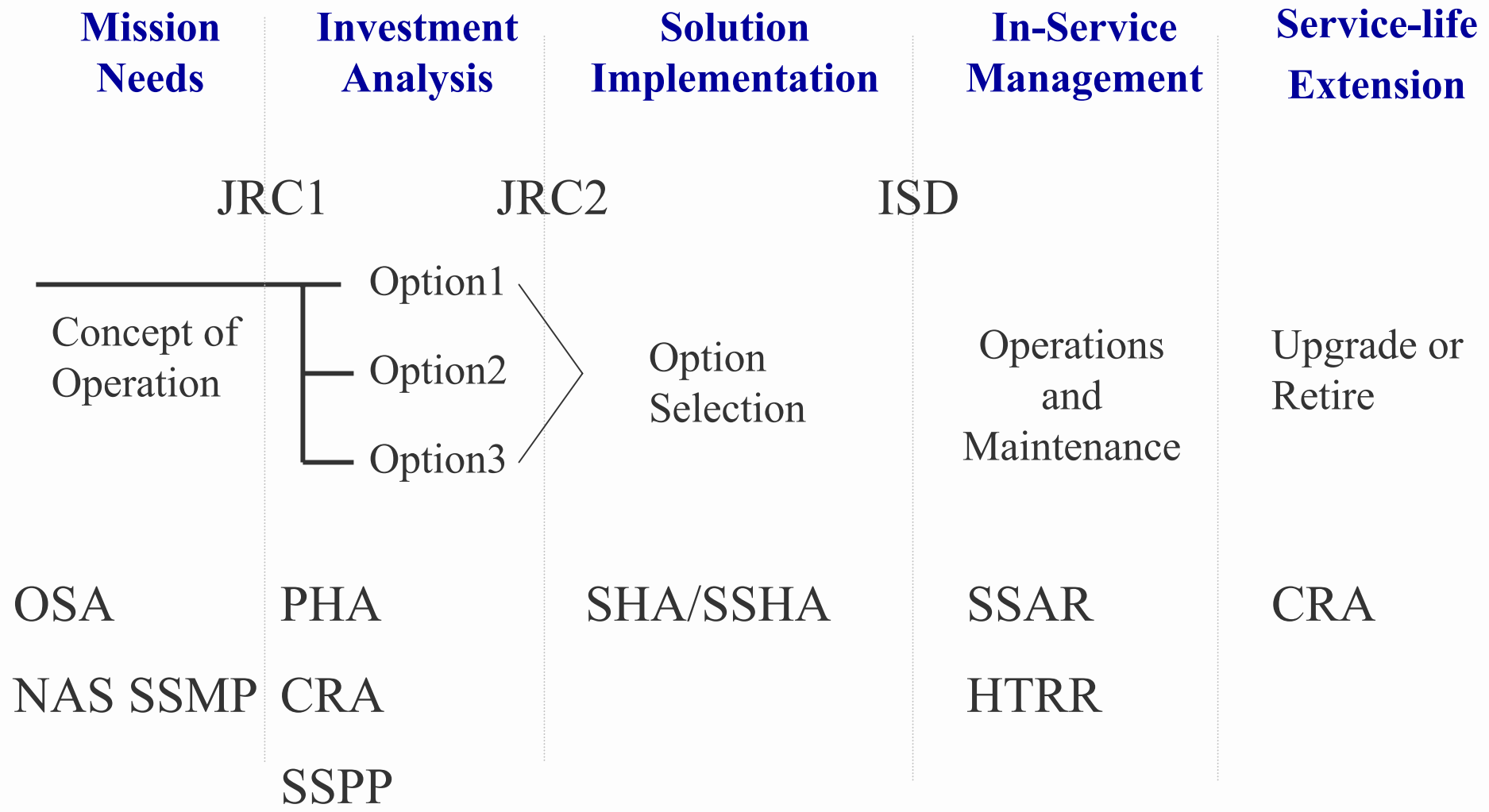
System Safety Working Group

- Purpose
  - Working arm of the System Engineering Council
  - Assists in supporting and evaluating Comparative and Operational Safety Assessments
- Products
  - System Safety Management Plan
  - System Safety Handbook

Acquisition Management System

- The FAA's Acquisition Management System (AMS)/Life-cycle Management System (LMS) consists of:
  - Mission Needs
  - Investment Analysis
  - Solution Implementation
  - In-Service Management
  - Service-life Extension

System Safety Process



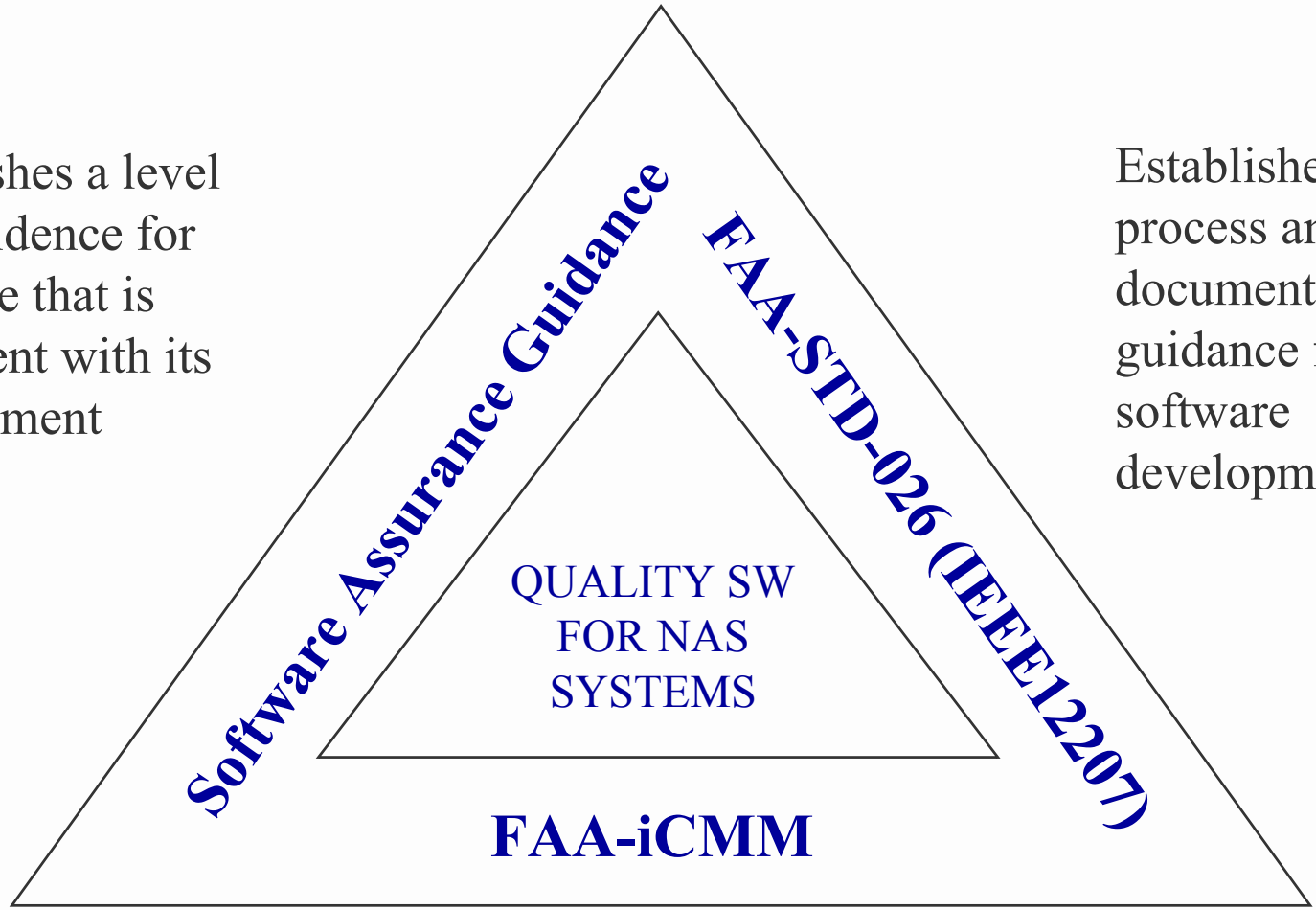
FAA CNS/ATM Software

- **FAA-iCMM**
- **Software development**
- **Software assurance**

Implement and integrate software engineering processes into systems engineering.

Software Quality Triangle

Establishes a level of confidence for software that is consistent with its environment



Establishes a process and documentation guidance for software development

Establishes essential elements of an organizations software acquisition, engineering, and management process

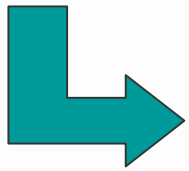
Software Assurance

- **What do we want to achieve?**

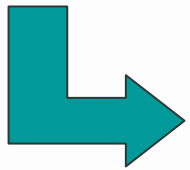
Identify the objectives necessary, throughout the life cycle process, to provide confidence that a product and process satisfies given safety and security integrity level requirements. ICAO has established a targeted Global Risk Factor of extremely remote or 10-7

Safety and Security Similarities

ANALYSIS



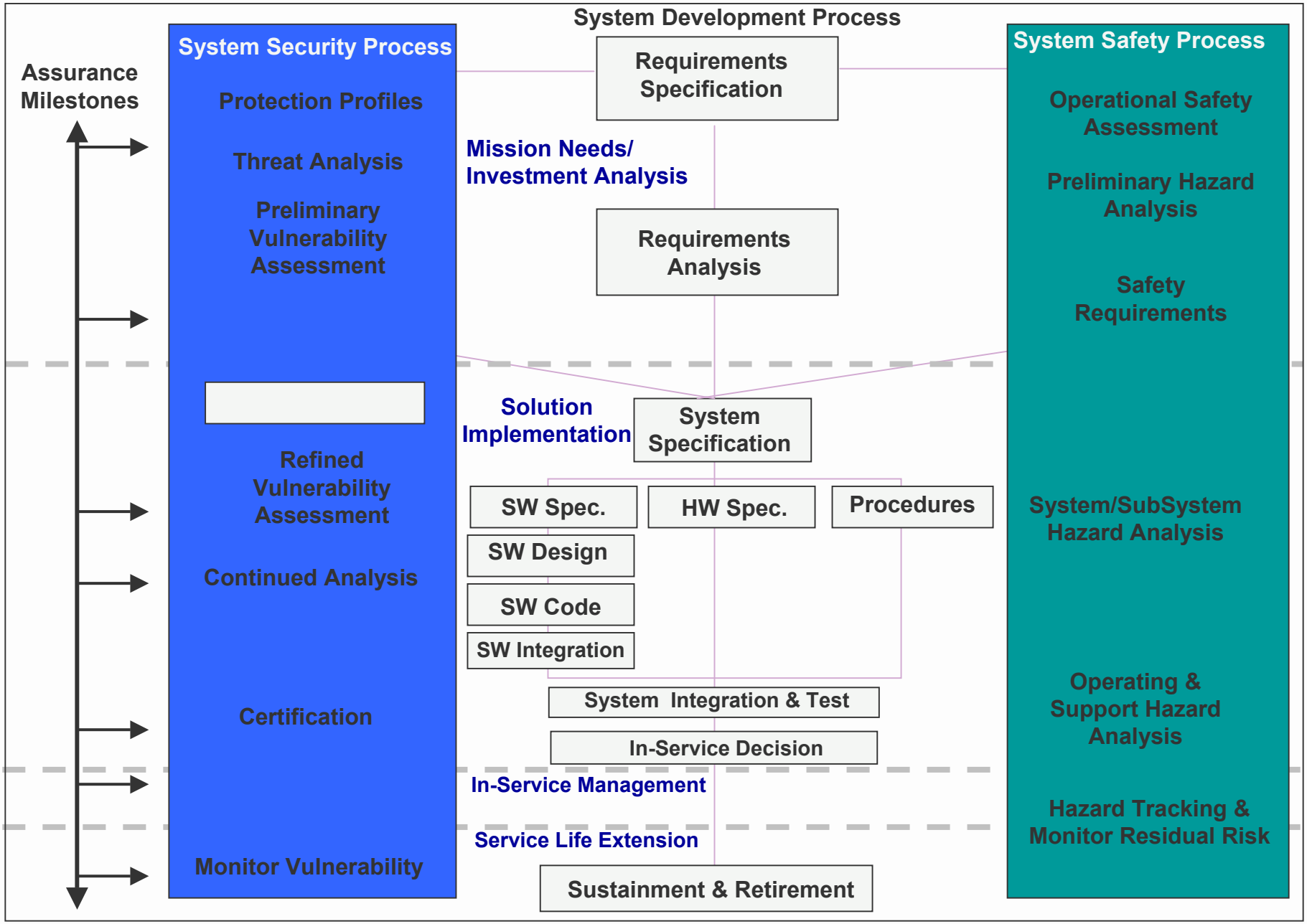
REQUIREMENTS



VERIFICATION

SECURITY	SAFETY
• Vulnerability/Threat Assessment	• Operational Safety Assessment
• Risk Determination	• Risk Determination
• Security Requirements	• Safety Requirements
• Penetration testing	• Requirements-based testing

Preliminary Safety/Security Model



Summary

- The FAA continues to refine its systems and software engineering processes
- We are focusing on the technical and programmatic efficiencies that can be achieved by integrating safety and security into the system life cycle processes.
- The FAA is present to gain knowledge and understanding from other industries on their approach to mitigating safety issues.

Backup slides

Acronyms (1/2)

- AMS Acquisition Management System
- CRA Comparative Risk Analysis
- FAA Federal Aviation Administration
- FMEA Failure Modes Effects Analysis
- HTRR Hazard Tracking and Risk Resolution
- ICAO International Civil Aviation Organization
- ISD In-service Decision
- JRC Joint Resource Council
- LMS Life-cycle Management System
- NAS National Airspace System

Acronyms (2/2)

- OSA Operational Safety Assessment
- PHA Preliminary Hazard Assessment
- SEMP System Engineering Management Plan
- SEM System Engineering Manual
- SHA System Hazard Analysis
- SSH System Safety Handbook
- SSHA SubSystem Hazard Analysis
- SSMP System Safety Management Plan
- SSAR System Safety Assessment Report